ShieldsUP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Checking the Most Common and Troublesome Internet Ports

This Internet Common Ports Probe attempts to establish standard TCP Internet connections with a collection of standard, well-known, and often vulnerable or troublesome Internet ports on **YOUR** computer. Since this is being done from **our** server, successful connections demonstrate which of your ports are "open" or visible and soliciting connections from passing Internet port scanners.

Your computer at IP:

38.172.64.208

Is being profiled. Please stand by. . .

Total elapsed testing time: 5.160 seconds

FAILED **TruStealth Analysis** FAILED

Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

Ping Reply: RECEIVED (FAILED) — Your system REPLIED to our Ping (ICMP Echo) requests, making it visible on the Internet. Most personal firewalls can be configured to block, drop, and ignore such ping requests in order to better hide

systems from hackers. This is highly recommended since "Ping" is among the oldest and most common methods used to locate systems prior to further exploitation.

Port	Service	Status	Security Implications
0	<nil>	Closed	Your computer has responded that this port exists but is currently closed to connections.
21	FTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
22	SSH	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
80	HTTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
110	POP3	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
119	NNTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
135	RPC	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
139	Net BIOS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
143	IMAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
389	LDAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
443	HTTPS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
445	MSFT DS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

1002	ms-ils	Closed	Your computer has responded that this port exists but is currently closed to connections.
1024	DCOM	Closed	Your computer has responded that this port exists but is currently closed to connections.
1025	Host	Closed	Your computer has responded that this port exists but is currently closed to connections.
1026	Host	Closed	Your computer has responded that this port exists but is currently closed to connections.
1027	Host	Closed	Your computer has responded that this port exists but is currently closed to connections.
1028	Host	Closed	Your computer has responded that this port exists but is currently closed to connections.
1029	Host	Closed	Your computer has responded that this port exists but is currently closed to connections.
1030	Host	Closed	Your computer has responded that this port exists but is currently closed to connections.
1720	H.323	Closed	Your computer has responded that this port exists but is currently closed to connections.
5000	UPnP	Closed	Your computer has responded that this port exists but is currently closed to connections.

Text Summary

You may click on the Text Summary button to receive a condensed textual report of the Common Ports Probe findings displayed above.

You may also click on any port number link above to jump to detailed information about that port contained in our Port Authority database.

For help and information about the meaning and importance of "Open", "Closed" and "Stealth" port statuses, please see our Internet Port Status Definitions page.

You may press your browser's BACK button to return to the previous page, Re-run the Common Ports Probe test by "refreshing" this page, or select from among the other services available:

Click here to check your router now...

GRC's Instant UPnP Exposure Test

You may select any service from among those listed above . . .

User Specified Custom Port Probe | Lookup Specific Port Information

Or enter a port to lookup, or the ports for a custom probe to check, then choose the service. Your computer at IP 38.172.64.208 will be tested.

Jump To Top